

**SUMMARY ANALYSIS OF AMENDED BILL**

Author: Simitian Analyst: Deborah Barrett Bill Number: SB 364  
 January 7, 2008 &  
 Related Bills: See Prior Analysis Telephone: 845-4301 Amended Date: January 17, 2008  
 Attorney: Tommy Leung Sponsor: \_\_\_\_\_

<b>SUBJECT:</b>	State Agencies Disclose Any Breach Of Security Of Data Systems That Contain Personal Information/Substitute Notices Allowed If Cost To Agency Exceeds \$100,000
_____	DEPARTMENT AMENDMENTS ACCEPTED. Amendments reflect suggestions of previous analysis of bill as introduced/amended _____.
_____	AMENDMENTS IMPACT REVENUE. A new revenue estimate is provided.
_____	AMENDMENTS DID NOT RESOLVE THE DEPARTMENTS CONCERNS stated in the previous analysis of bill as introduced/amended _____.
_____	FURTHER AMENDMENTS NECESSARY.
_____	DEPARTMENT POSITION CHANGED TO _____.
<u>X</u>	REMAINDER OF PREVIOUS ANALYSIS OF BILL AS INTRODUCED <u>February 20, 2007</u> , STILL APPLIES.
_____	OTHER – See comments below.

**SUMMARY**

This bill would reduce the cost threshold under which state agencies can elect to provide substitute notice in the event of a breach of security of data systems containing personal information and would require notice of the breach to be provided to the Office of Privacy Protection (OPP).

**SUMMARY OF AMENDMENTS**

The January 7, 2008, amendments revised the notification requirements for a breach of security of a system containing personal information to require a notification to be sent electronically to OPP. The January 7, 2008, amendments also require OPP to make publicly available, on their Web site, copies of the notifications received, as well as reducing the threshold cost amount for which substitute notice is required under the bill from \$250,000 to \$100,000.

The January 17, 2008, amendments revised the threshold cost amount for which substitute notice is required under this bill back to \$250,000, and made an additional nonsubstantive technical change. The "Current Law," "This Bill," "Program Background," and "Implementation Concerns" discussions have been revised and are included in the analysis below. The remainder of the department's analysis of the bill as introduced February 20, 2007, still applies.

Board Position:			Legislative Director	Date
_____ S	_____ NA	_____ NP	Brian Putler	1/30/08
_____ SA	_____ O	_____ NAR		
_____ N	_____ OUA	<u>X</u> PENDING		

## **POSITION**

Pending.

## **ANALYSIS**

### **STATE LAW**

Under current state law, any state agency that owns or licenses computerized data that includes personal information and that experiences a breach of security of the system containing that data must notify the affected individuals that their unencrypted information may have been or is reasonably believed to have been acquired by an unauthorized person. Notification of the breach of security can be provided by written notice, by electronic notice, or by substitute notice if the cost of providing the notice would exceed \$250,000 or involves a class of affected persons in excess of 500,000 persons. Substitute notice can be accomplished by e-mail notification, by posting of the notice in a conspicuous place on the agency's Web site, or by notifying major statewide media.

Existing state law prohibits the disclosure of any taxpayer information, except as specifically authorized by statute. Generally, disclosure is authorized to other state tax agencies, federal tax agencies, other state tax agencies, and the Multi-State Tax Commission for tax administration purposes only. Other exceptions are specified in statute. Unauthorized disclosure of state tax information is a misdemeanor and improper disclosure of federal tax information is a felony.

The Statewide Information Management Manual (SIMM) requires agencies with systems that maintain personal information to provide an incident report within ten days to the California Highway Patrol and OPP if a breach of the system has occurred.

### **THIS BILL**

This bill would require any agency that owns or licenses computerized data that includes personal information and that experiences a breach of security of the system containing that data must notify the affected individuals that their unencrypted information may have been or is reasonably believed to have been acquired by an unauthorized person. Notification of the breach of security can be provided by written notice, by electronic notice, or by substitute notice if the cost of providing the notice would exceed \$100,000 or involves a class of affected persons in excess of 500,000 persons. Substitute notice can be accomplished by e-mail notification, by posting of the notice in a conspicuous place on the agency's Web site, or by notifying major statewide media.

In addition to notifying the affected person, agencies are required to provide the Office of Privacy Protection (OPP) with a copy of the notification of a breach of system security that is sent to California residents.

OPP is required to establish a process by which agencies can electronically provide notification to OPP, and is required to establish a Web site to make notifications public record. The notice is required to contain the following information:

- The toll-free telephone numbers and addresses of the major credit reporting agencies.
- The name and contact information of the reporting agency.
- A list of the types of information, such as name or social security number, that may have been subject of a breach.
- The date of a breach, if known and the date of discovery of a breach, if known.
- The date of the notification and whether the notification was delayed pursuant to law enforcement direction or other permissible delays.
- A general description of the breach incident.
- The estimated number of persons affected by the breach.
- Whether substitute notice was used.

OPP is required to report annually to the Legislature a summary of the information collected and made available via the Web site prescribed in this bill.

## **PROGRAM BACKGROUND**

The notice Franchise Tax Board (FTB) sends to inform a taxpayer of a breach of security involving personal information includes the use of the mailing address of the taxpayer that is obtained from confidential tax returns. Because current law prohibits FTB from disclosing confidential tax information for purposes other than tax administration, FTB would not be able to use its current notification format to provide OPP notice of the breach as required by this bill.

## **IMPLEMENTATION CONSIDERATIONS**

To accommodate the requirements of this bill and adhere to existing disclosure restrictions, Franchise Tax Board would revise current notification formats to separate the confidential tax information used to correspond with the taxpayer from the notification of the breach of security that would be provided to OPP for publication. This revision to current practice could be accomplished within the department's annual updates

This bill would require any security breach notification sent to California residents to also be sent electronically to OPP. The language is vague for instances of a breach involving multiple residents whether one notification of the incident is sufficient or whether the author intends state agencies to send multiple notices of the same incident to OPP. For instance, if 1,000 residents are involved, would 1,000 separate notices be sent to OPP or would one notice detailing the incident size of 1,000 be sufficient for the author's purposes. Clarification would assist the department to implement this bill.

Because current SIMM instructions require agencies that maintain systems containing personal information to provide an Incident Report to OPP within ten days of the incident, the similar provisions of this bill as they relate to state agencies are duplicative.

#### **LEGISLATIVE STAFF CONTACT**

Analysis prepared by  
Deborah Barrett  
(916) 845-4301  
[Deborah.Barrett@ftb.ca.gov](mailto:Deborah.Barrett@ftb.ca.gov)

Revenue estimated by  
Keith York  
(916) 845-5299  
[Keith.York@ftb.ca.gov](mailto:Keith.York@ftb.ca.gov)

Brian Putler  
Franchise Tax Board  
(916) 845-6333  
[brian.putler@ftb.ca.gov](mailto:brian.putler@ftb.ca.gov)